EXPRESS MAIL NO. EK555899074US

PATENT
Attorney Docket No.: 00-4069

Patent Application Filed

UNITED STATES PATENT APPLICATION

FOR

QUANTUM CRYPTOGRAPHIC KEY DISTRIBUTION NETWORKS WITH UNTRUSTED SWITCHES

BY

BRIG BARNUM ELLIOTT

DESCRIPTION OF THE INVENTION

Cross-Reference to Related Applications

[0001] The instant patent application claims the benefit of U.S. Provisional Patent Application Serial No. 60/242,597, filed October 23, 2000, which is hereby incorporated by referenced in its entirety. The instant patent application is related to co-pending Attorney docket No. 01-4015, U.S. Patent Application Serial No. _____, entitled "SYSTEMS AND METHODS FOR PATH SET-UP IN A QUANTUM KEY DISTRIBUTION NETWORK," filed on even date herewith, having assignee in common with that of the instant patent application, which is incorporated herein by reference in its entirety.

Field of the Invention

[0002] The present invention relates to methods and systems for using the principles of quantum mechanics to distribute a random cryptographic key over an insecure network using untrusted switches.

Description of Related Art

[0003] Cryptography is the science of securing information by rendering it unreadable to everyone except the intended recipient of the information. Cryptography also provides a mechanism to ensure that a message is authentic and unmodified. Information that has been cryptographically rendered unreadable may be described as "encrypted," and conversely, unreadable information that is unscrambled and again rendered into readable form may be described as "decrypted." The process of encrypting and decrypting information using traditional cryptographic methods employs at least one piece of information commonly called a "key" because it is used to "unlock" an encrypted message. Cryptography has traditionally been

of great importance to persons seeking to communicate secretly. Applications of cryptography range from the protection of private records to secure payment systems.

[0004] Symmetric cryptography describes a system of encrypting and decrypting information using the same key to perform both encryption and decryption. There are numerous symmetric cryptographic methods, having various characteristics including relative strength, speed of computation, and convenience. The one-time pad offers security that is considered to be unbreakable. However, all symmetric cryptographic methods share a common problem, namely the need to privately and securely exchange information about the symmetric key.

[0005] Secure key exchange methods are used to exchange cryptographic keys. A traditional solution to this problem is to physically deliver the key via a secure courier. Another method is to use public key cryptography to exchange a symmetric key. Methods of public key cryptography are well known. Yet another method for securely exchanging keys is quantum cryptography.

[0006] Quantum cryptography is a technique for the private and secure distribution of a key for use in subsequent encryption and decryption. Quantum cryptography is built upon the principles of quantum mechanics, according to which there is statistical uncertainty regarding the properties of a photon. Furthermore, principles of quantum mechanics require that the act of observing a series of randomly oriented photons necessarily will affect some of the observed photons. This principle is used in quantum cryptography to securely exchange keys, because in

observing the states of the transmitted photons, an eavesdropper will detectably corrupt the states of the transmitted photons.

[0007] In the field of quantum cryptography, there has been significant research, resulting in a number of publications and issued patents. In a well-known publication by Charles H. Bennett and Gilles Brassard, entitled "Quantum Cryptography: Public Key Distribution and Coin Tossing", International Conference on Computers, Systems & Signal Processing, Bangalore, India (1984), Bennett and Brassard describe a quantum-cryptographic system in which a random key is transmitted using photons having random orientations. A receiver observes the photons with a randomly oriented basis, recording the orientations of the receiver basis and the observed photons. In a separate public channel that may be subject to passive eavesdropping, the sender and receiver then compare and discard a random subset of the transmitted bits to determine whether there had been significant errors or eavesdropping in the quantum channel. If the sender and receiver determine that a sufficiently small number of the compared bits were wrong, the remaining bits are used as key information for conducting encrypted communications on the public channel. The Bennett and Brassard system can withstand passive eavesdropping, i.e. listening in the public channel, but it cannot tolerate active eavesdropping, i.e. man-in-the middle attacks in the public channel.

[0008] Other research has resulted in more efficient methods of performing quantum-cryptographic ("QC") key exchange. For example, U.S. Patent No. 5,732,139 to Lo et al. ("Lo") describes an improved system relating to the selection of probabilities of the states of transmitted

photons, resulting in a reduced quantity of discarded data. However, Lo does not suggest a way to perform QC key exchange using untrusted networking switches.

[0009] These publications illustrate various techniques for using quantum cryptography, but they also illustrate one of its main shortcomings. Quantum cryptography is primarily a point-to-point key distribution technique, and when an intermediate piece of networking equipment such as a switch is introduced into a quantum cryptography path, the operator of the networking equipment can undetectably break the security of the key exchange. Therefore, all known systems employing quantum cryptography require the use of trusted switches. However, in practical networking environments, it is not economically feasible to have physical control of all components in a network. In practice, parts of a network may be controlled by enemies or competitors. Therefore, there is a need in the art for a system for securely employing quantum cryptography over a network including untrusted switches.

[0010] QC key distribution uses individual photons to convey keying information between two devices. In conventional QC techniques, these two devices are directly connected by an optical path, either via directly attached fiber that runs between the devices, or by free-space optical paths. In essence, one device sends a stream of individual photons directly from itself to another device. Then various protocols are used in order to agree on the quantum state conveyed via these photons and hence to agree on shared keying data. A very high degree of protection is provided by quantum cryptography - in essence, QC key distribution techniques make it impossible for an eavesdropper to gain information about the exchanged cryptographic key without being detected.

[0011] Conventional QC technology has the severe drawback, however, that it is a point-to-point key distribution technique. Therefore, known systems require intervening network devices to be brought into the same trust domain as the endpoint devices, meaning that the network devices must participate in and understand the key distribution process. This is undesirable in many ways, as systems are generally much more secure when users can employ encryption techniques that do not require trusted active participation of additional entities.

[0012] Micro-Electro-Mechanical Systems ("MEMS") comprising mirror arrays are used to perform optical switching in an optical networking environment. This technology is described in U.S. Patent No. 5,960,133 to Tomlinson ("Tomlinson"), entitled "Wavelength-Selectable Optical Add-Drop using Tilting Micro-Mirrors." Tomlinson further identifies publications disclosing the necessary technology for fabricating such devices, but Tomlinson fails to suggest the use of such technology in a system for performing quantum cryptographic key exchange.

[0013] Other publications have suggested that MEMS technology is ripe for use in telecommunications applications. See e.g. J. A. Walker, "Telecommunications Aspects of MEMS," International Newsletter on Microsystems and MEMS, No. 3/00, June 2000, pp. 6-9. In this article, Walker describes several applications of MEMS in optical fiber telecommunications systems, including optical cross-connects ("OXC") and the Lucent ™ WaveStar ™ Lambda Router, however, he does not suggest that MEMS technology be combined with quantum cryptography.

[0014] In addition to MEMS mirror arrays, there are other means of redirecting optical energy. U.S. Patent No. 5,960,131 to Foquet et al describes a switching mechanism for selectively connecting a first optical path to a second optical path through an index-matching fluid. U.S. Patent No. 6,005,993 to Robert I. McDonald discloses an optical switch that uses prisms to deflect and reflect optical energy so as to switch optical energy from input ports to output ports. U.S. Patent No. 6,154,586 to Robert I. McDonald et al. describes a switch mechanism having a block made of a light transmissive substrate containing a cavity that is divided by a light transmissive diaphragm into a reflective portion and a transmissive portion. U.S. Patent No. 5,911,018 discloses an optical switch element that uses wave-guide segments to switch optical energy from an input port to an output port. U.S. Patent Nos. 5,960,131, 6,005,993, 6,154,586,and 5,911,018 are incorporated herein by reference.

[0015] Multi-Protocol Lambda Switching ("MPL(ambda)S") is an optical networking technology using Multi-Protocol Label Switching ("MPLS") to provision OXCs. This work is being standardized in the Internet Engineering Task Force ("IETF"). See the IETF Draft entitled, " Multi-Protocol Lambda Switching: Combining MPLS Traffic Engineering Control With Optical Crossconnects, " by D. Awduche et al. (January 2001). Additional MPLS background is provided in "MPLS: Technology and Applications", by Bruce S. Davie and Yakov Rekhter, Morgan Kaufman Publishers (2000).

[0016] Communications network technology is very widely known to those of ordinary skill in the art. It is evident to those skilled in the art that traditional networking technology would be

greatly enhanced and benefited by a system for using quantum cryptography on untrusted switches.

SUMMARY OF THE INVENTION

[0017] Consistent with the present invention, methods and systems are provided by which a number of quantum-cryptographic endpoints, such as, for example, computers and firewalls, can be placed into a shared key distribution network and can exchange QC photons across a network without the network switches being able to read or alter the photons. The present invention provides the benefits of a shared key distribution network without requiring trusted switches.

[0018] In accordance with the present invention, methods and systems for securely transmitting information in a network comprising untrusted network components are provided. The methods and systems send at least one setup message to a networking device. Based on the setup message, the methods and systems configure at least one mirror device to direct polarized light along a path to a terminal endpoint, whereby a configured path is established. The methods and systems send a stream of bits using a plurality of polarized light pulses along the configured path, the pulses having a first set of randomly selected polarization bases. The methods and systems involve measuring the polarization of the polarized light pulses using a second set of randomly selected polarization bases.

[0019] Additional benefits of the present invention will be set forth in part in the description, which follows, and in part will be obvious from the description, or may be learned by practice of

the present invention. The benefits of the invention will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims.

[0020] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate exemplary embodiments consistent with the present invention and together with the description, serve to explain the principles of the present invention. In the drawings,

[0022] Figure 1 is block diagram illustrating a network in which systems consistent with the present invention may operate;

[0023] Figure 2 is a block diagram illustrating a key distribution path consistent with the present invention, the path passing through a network of untrusted switches;

[0024] Figure 3A is a block diagram illustrating an optical-fiber network path consistent with the present invention through a network, including networking switches;

[0025] Figure 3B is a block diagram illustrating a quantum cryptographic key exchange consistent with the present invention in a network using micro-electro-mechanical systems;

[0026] Figure 4 is a block diagram illustrating a networking switch consistent with the present invention;

[0027] Figure 5 is a flow diagram illustrating steps performed by an ingress switch consistent with the present invention;

[0028] Figure 6 is a flow diagram illustrating steps performed by an intermediate switch in a network consistent with the present invention;

[0029] Figure 7 is a flow diagram illustrating steps performed by networking devices in a setup phase consistent with the present invention; and

[0030] Figure 8 is a flow diagram illustrating steps performed by networking devices in a circuit-tear-down phase consistent with the present invention.

DETAILED DESCRIPTION

Network Description

[0031] The present invention provides a highly secure key-distribution system within a potentially insecure optical-fiber network, using untrusted switches to form secure links, based on the principles of quantum cryptography. An untrusted switch is a switch that is operated by

or accessible to a party that may attempt to eavesdrop on or intercept network communications. The untrusted switches are unable to read or alter the contents of any communication between endpoint devices because the switches passively redirect light from one fiber strand to another using OXC or other technology for redirecting optical energy. QC principles prevent undetected eavesdropping in the optical channel.

[0032] This is an extremely useful result as it provides a highly secure key-distribution infrastructure that can be employed by one organization using fiber optics maintained by another organization. For example, a network within a classified government facility could securely convey cryptographic key data for several different "compartments" of traffic. Each compartment would be strictly isolated from each other and from the underlying switching infrastructure. As another example, a metropolitan area network, using technology consistent with the present invention, could act as the key distribution infrastructure for a number of competing companies while protecting the confidential business information in each company. Each company would be able to securely distribute keys over the shared optical-fiber network without concern that the company's cryptographic keys were being intercepted, monitored, or altered by another entity using the same metropolitan network.

[0033] In accordance with the present invention, endpoint devices send and receive single photons or light pulses having characteristics similar to single photons. The endpoints use these photons to convey keying information. In one embodiment, the switches employ MEMS technology to provide a set of reflective devices that reflect the photons from an origin endpoint to a terminal endpoint, possibly passing through multiple switches, consistent with the present

invention. Alternatively, instead of MEMS reflectors, the switches may employ other reflective devices, such as for example conventional mirrors, optics, photonic-band-gap material, and other known optical switching devices. Because these reflective devices are passive reflectors, they cannot read or alter the photons' quantum state. Hence the switches are not part of the trust domain; the photons are created and observed only at endpoint devices, and if a switch attempts to observe the photons, the observation will be detected, consistent with known QC principles.

[0034] Networking technology exists that is capable of realizing switches, consistent with the present invention. In fact, production optical switching networks that use OXC are beginning to be deployed. Systems and methods consistent with the present invention leverage this new field of commercial technology to provide new systems for quantum cryptographic key distribution.

[0035] Figure 1 is block diagram illustrating a network in which systems consistent with the present invention may operate. Switches, such as switches 110, 112, 114, 116, 118, 120, and 122 are illustrative untrusted switches within the network of Figure 1. User endpoints are represented by the circular endpoints 102, 130, and 140. These endpoints are representative of individual computer systems such as personal computers, web servers or other computer systems that need to privately exchange cryptographic key data. Endpoints 120, 130, and 140 may be also representative of logical network-demarcation points, such as for example, firewalls. In Figure 1, solid lines, such as network connection 132 represent optical fiber connections that may be used for quantum cryptographic key distribution. The dotted lines, such as network connection 134 represent a specific path taken by a stream of photons, from endpoint 130 to endpoint 140. This path passes through a series of intermediate untrusted switches, in this case

switches 110, 114, 118, and 122. The path through these untrusted switches forms a QC key distribution path between endpoints 130 and 140.

[0036] In Figure 1, multiple switches are shown, however, in another embodiment, consistent with the present invention, key information may be securely exchanged over a simpler network in which a number of endpoints are directly connected to a single switch, forming a star topology. In this embodiment, a number of computers in a single building form highly secure associations between pairs of computers so that only the particular computers involved in a chosen association participate in a secure communication session.

[0037] Figure 2 is a block diagram illustrating a key distribution path consistent with the present invention, the path passing through a network of untrusted switches. In one embodiment, computers 260 and 270 are equipped with a quantum cryptographic key distribution interface as used in quantum cryptography. Three switches are also shown, namely switches 210, 220 and 230. In this embodiment, quantum photons are sent from computer 260 through switches 210, 220, and 230 to computer system 270. Along this path, photons are directed by MEMS mirror arrays 212, 222, and 232, in switches 210, 220, and 230 respectively. Thus individual photons travel from endpoint computer 260 to endpoint computer 270 without being inspected, altered, amplified, or regenerated in any way by switches 210, 220, and 230.

[0038] In an embodiment, consistent with the present invention, a path through a quantum cryptographic network is established by properly arranging optical switching devices, such as, for example, mirrors in MEMS arrays, so that photons travel from computer 260 to computer

270. The mirror arrangement process is coordinated by a series of control or setup messages that travel along setup network connections 250, 252, and 254. The setup messages are sent using known protocols such as, for example, the Constraint-based Routing Label Distribution Protocol ("CR-LDP") or the Resource Reservation Protocol ("RSVP"). The messages are exchanged between endpoint devices via intermediate network switches. The setup messages contain information necessary to adjust the optical switching device configuration, producing path 240, along which photons can travel. Thus established, path 240 becomes a trusted path through untrusted network devices. Not shown in Figure 2 is a separate, conventional network path, which is used for the transmission of data messages and for the public portion of QC key distribution. The conventional path may be implemented using known means, such as, for example, IP datagrams, ATM, or SONET. Consistent with the present invention, quantum cryptographic methods are used to exchange key information over the QC fibers, after which secure communication can proceed using known cryptographic methods on the conventional network.

[0039] Figure 3A is a block diagram illustrating an optical-fiber network path consistent with the present invention through a network, including networking switches. The switches are interconnected via a number of parallel optical fibers, e.g. as deployed in conventional fiber cables which often have 48 or more fibers in a single cable. The pathway between origin endpoint 330 and terminal endpoint 340 is set up along unused fibers throughout path so that each QC photon travels along a dedicated set of fibers. An individual fiber is allocated to a single QC key exchange session. Switches 310, 312, and 314 determine a path from origin endpoint 330 to terminal endpoint 340, using currently unused fibers. This function is very similar to

known methods of establishing paths, using protocols such as MLPLS and MPL(ambda)S. Therefore routing and path setup techniques can be borrowed from those proven technologies, as will be appreciated by those of ordinary skill in the art.

[0040] Each QC photon emerges from an inbound fiber into a switch, and the switch redirects the photon using an optical switching device, such as, for example, a small mirror that is precisely angled so as to direct the photon into a predetermined outbound fiber. In this way, individual QC photons travel through the network from origin endpoint 330 to terminal endpoint 340.

[0041] Figure 3B is a block diagram illustrating a quantum cryptographic key exchange consistent with the present invention in a network using MEMS. In this embodiment, quantum cryptographic transceiver 350 transmits a QC photon over link 352. MEMS mirror element 354 directs the QC photon through a path along an optical fiber network terminating via link 356 at quantum cryptographic transceiver 360.

[0042] Figure 4 is a block diagram illustrating a networking switch consistent with the present invention. The switch is controlled by central processing unit ("CPU") 410. CPU 410 may be one of the commercially available microprocessors or microcontrollers, such as, for example the MC68302 from Motorola Inc. Memory 420 is used to store the instructions for causing CPU 410 to perform methods consistent with the present invention. Memory 420 may also include buffer space used to store state variables used in performing such methods. Memory 420 may be implemented using RAM, ROM, EEPROM, Flash EEPROM and equivalent devices.

Network interface 430 is used to connect the switch to a conventional network for the exchange of setup and configuration information within the network. MEMS mirror array 440 is connected to bus 450 that interconnects array 440 with CPU 410, memory 420, and network interface 430.

Path Formation

[0043] In order to facilitate the secure exchange of cryptographic key data over QC networks, consistent with the present invention, a QC path must be formed between an origin endpoint and a terminal endpoint. The present invention relies on the use of a circuit-switched network, and the operation of circuit-switched networks involves several processes, including: circuit setup, communication, and circuit teardown. Methods and systems consistent with the present invention use known circuit-switching techniques to provide a new way to perform QC key exchange via untrusted switches, and, since circuit-switching operations are known, general circuit operations will not be described in great detail.

[0044] Figure 5 is a flow diagram illustrating steps performed by an ingress switch consistent with the present invention. An ingress switch is the switch into which a QC photon enters a switched network. On a conventional public network, the ingress switch receives a setup message from an originating endpoint computer (step 510). Next, the ingress switch uses known methods to determine a path to the terminal endpoint (step 520). In one embodiment, the switch accesses records in an internal network topology database to determine a complete path to the terminal endpoint, i.e., a path that has unused fiber segments for the entire path to the terminal switch. In this embodiment, the switch makes an internal record in its memory of which outbound fiber segment it will use for the current QC connection. In other embodiments

individual switches do not maintain complete path information, instead relying on the routing techniques inherent in a protocol, such as, for example, label switching.

[0045] Next, the switch adjusts its internal optical switching devices to passively redirect incoming photons from the originating endpoint computer to a fiber strand that forms a path to the next device in the network (step 530). Finally, on the conventional network, the switch forwards to the next device in the network path an intermediate setup message, such as for example, a label routing message (step 540). In one embodiment, the setup message is augmented with information on a complete source route from the ingress switch to the terminal endpoint, i.e., a list of all switches that must be traversed.

[0046] Figure 6 is a flow diagram illustrating steps performed by an intermediate switch (e.g. switch 114 or switch 118 of Figure 1) in a network consistent with the present invention. An intermediate switch receives a setup message from an upstream neighbor switch in the network and removes itself from the label routing information within the setup message (step 610). Next, the intermediate switch chooses an outbound fiber based on information obtained from the setup message (step 620). In one embodiment, the intermediate switch makes an internal record regarding the outbound fiber segment it selected for the outbound connection. Next, the intermediate switch adjusts its optical switching device so that photons from the incoming fiber are directed into the newly allocated outbound fiber segment (step 630). Next, the intermediate switch sends the revised setup message to the next downstream switch (possibly another intermediate switch) or to the terminal endpoint, if the intermediate switch is an egress switch (step 640).

[0047] Figure 7 is a flow diagram illustrating steps performed by networking devices in a setup phase consistent with the present invention. Once a complete set of setup messages have traversed the path of network switches to the terminal endpoint, the terminal endpoint device prepares to accept QC photons from the origin endpoint device. The terminal endpoint device sends an accept or reject message along the reverse path of the connection setup (step 710). And each switch along the path inspects the accept or reject message. If the message is a reject message (step 720), then a circuit teardown operation begins (step 750), as further described in connection with Figure 8. After the teardown operation is completed, the switch forwards the reject message to the next upstream switch (step 760). If, however, the terminal endpoint sent an accept message, the receiving switch confirms that its optical switching device is properly set up (step 730). Finally, the receiving switch forwards the confirmation message to the next upstream switch or to the origin endpoint if the receiving switch is the ingress switch (step 740).

Quantum-Cryptographic Communication

[0048] Next the origin and terminal endpoints exchange cryptographic key information using known QC techniques, such as described above and in U.S. Patent No. 5,764,765 to Phoenix et al., which is incorporated herein by reference. During this phase the endpoint devices may be oblivious to the fact that the photons used in these operations are bouncing along a series of mirrors and traveling through fiber segments in traversing the path from origin endpoint to the terminal endpoint.

[0049] Sending and receiving photons over network paths, consistent with the present invention, may be performed using available telecommunications equipment. For example, D. S.

Bethune and W. P. Risk describe systems for sending and receiving QC signals in "An Autocompensating Fiber-Optic Quantum Cryptography System Based on Polarization Splitting of Light," IEEE Journal of Quantum Mechanics, Volume 36, Number 3, March 2000, at. 340, which is incorporated herein by reference. Bethune and Risk explain that single photons having wavelengths of 1.31 and 1.55 μm can be detected using Ge or InGaAs avalanche photodiodes ("APD"), such as, for example, Fujitsu ™ FPD5W1KS InGaAs APD's. Consistent with the present invention, polarized light pulses may be generated using standard telecommunications lasers and standard polarizing beam splitters. One embodiment consistent with the present invention uses the above technology disclosed by Bethune and Risk, however, the invention is not limited to these devices, and equivalents may be employed and substitutions made without departing from the scope of the present invention as recited in the claims. For example, instead of polarization states of photons, the relative phase between two amplitude packets, produced by splitting each light pulse and delaying one portion before sending it, may be used to communicate a stream of bits for QC key distribution.

Quantum-Cryptographic Link Teardown Phase

[0050] Figure 8 is a flow diagram illustrating the steps performed by networking devices in a circuit-tear-down phase consistent with the present invention. Upon completion of key exchange, or when either endpoint device chooses to terminate the QC connection, link teardown proceeds as follows. The terminating endpoint composes a "DONE" message and sends the message to its attached switch (step 810). The attached switch resets the associated MEMS mirror for this connection to an idle position (step 820). In one embodiment, the switch marks the associated outbound fiber segment as unused in its internal database. Next, the switch

determines if it is the last switch in the path (step 830), and if it is the last switch, the method terminates, otherwise, the method continues at step 810.

[0051] Since there are known methods for establishing circuits in a network, it is not necessary to further explain the process by which switches, consistent with the present invention, communicate setup information regarding free and in-use fiber segments within the network. For example, circuit switching techniques consistent with the present invention are similar to the techniques used in MPLS for finding free capacity for new traffic circuits, to those used in MPL(ambda)S for finding free wavelengths across Dense Wavelength Division Multiplexing ("DWDM") networks, and to those used for routing in Asynchronous Transfer Mode ("ATM") networks. As such, the CR-LDP or Private Network-to-Network Interface ("PNNI") protocols provide the necessary technological framework for the establishment of the fiber connections needed in systems consistent with the present invention. Known protocols for circuit-switch construction may be implemented with only minor modifications that may be appreciated through practice of the invention.

Alternative Embodiments

[0052] Illustrative embodiments have been described, in connection with multiple fiber segments between network switches, however there are alternative embodiments. Instead of using parallel fibers, individual wavelengths within a single fiber may be used for the quantum communications channels. This embodiment leverages Dense Wavelength Division Multiplexing ("DWDM") technology. In this embodiment, a single frequency band is reserved along the entire path from an origin endpoint to a terminal endpoint. The endpoints tune lasers and photon detection devices to an appropriate frequency before exchanging QC photons. In this

embodiment, unlike conventional, electro-optical, DWDM networks, photons are not regenerated at each switch. Thus a single wavelength must be reserved from endpoint to endpoint.

[0053] In another alternative embodiment, time division multiplexing ("TDM") is used in the fiber strands instead of wavelength division multiplexing. In this way, a number of different QC sessions may be multiplexed onto a single fiber by ensuring that the endpoints are time-synchronized and that each set takes a turn using the fiber. TDM further involves additional synchronization throughout the network; essentially it requires "coloring the topology graph" in order to determine free times at which a given device may transmit a photon so that it does not interfere with any other device's use of any of the fiber segments along the path. TDM also requires re-adjusting the mirrors along the path at each time slice.

Conclusion

[0054] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. Principles of quantum mechanics are not limited to any portion of the electromagnetic spectrum. Accordingly, embodiments of the present invention are not constrained to operate only within limits of the human-visible spectrum. Therefore, the terms "light" and "light information", as used and claimed herein, are not necessarily referring to phenomena falling only within the human-visible light spectrum. These terms can be referring to phenomena occurring both within the infra-red and/or ultraviolet limits to the human-visible spectrum and beyond such limits as well. Moreover, quantum principles also apply to physical phenomena other than photons, for example, to entire atoms or their constituent components. Therefore, "light" should be understood in the broad sense of physical waves or particles, rather than its more restricted sense

of photons. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

Filed: 8 December 2003